KETS

Google Apps SSO to Office 365 Integration

Kentucky Department of Education

Version 1.5 12/3/2014

Google Apps for Education (GAFE)

+

Microsoft Active Directory Integration

Introduction

Welcome to the Google Apps for Education (GAFE) authentication integration into Office 365. This guide outlines the technologies and steps involved in the initial configuration of your district's GAFE environment to leverage the login credentials of Office 365. It also contains the support 'triage' for ongoing support of this configuration.

Audience

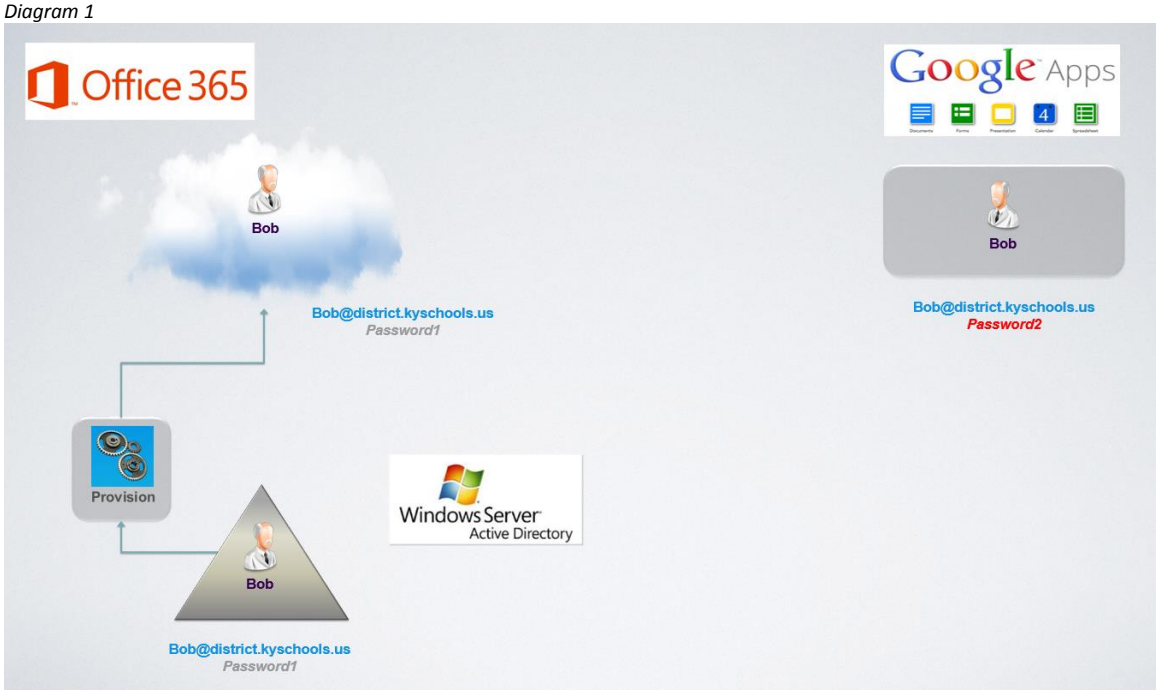
This guide was written and is kept up-to-date for the technical administrators of Kentucky school districts' Office 365 environment and Google Apps for Education suite.

Technologies/Terminologies

There are acronyms and technology terms that are used when discussing user access to technology systems. This section will attempt to define terminology used in this guide as well as provide a high-level overview of the major components that comprise user access, as these pertain to this discussion.

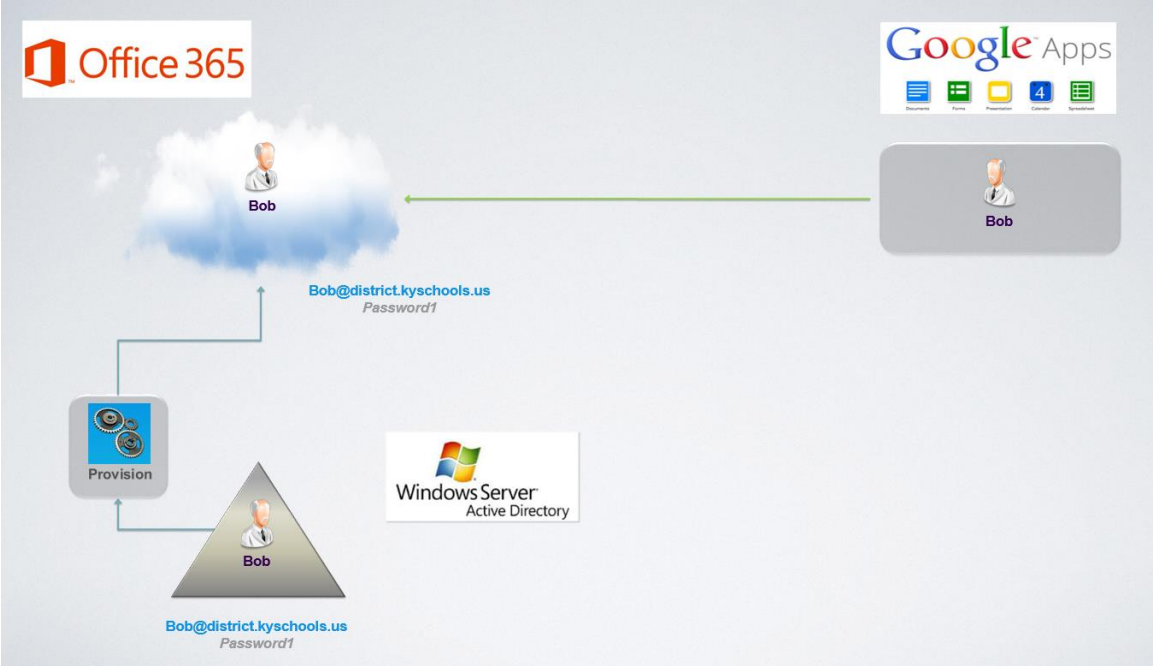
Single Sign-On (SSO) is the ability to utilize one set of login credentials for two or more systems. In this scenario the Office 365 credentials would be the authority for login access into Google Apps. In the KETS environment the Office 365 login creds are also the same as the Active Directory credentials. Prior to the implementation of your GAFE environment to use SSO with Office 365, the user login experience is either a different password for GAFE than Office 365, or a manual process of setting the password the same in GAFE as Office 365. The diagram below is a simple representation of the separate Google Apps environment from AD and Office 365.

Diagram 1



Authentication into any system simply validates a user's identity. It by itself gives them no access to anything, it just proves they are who they say they are when 'logging in'. It is like showing a photo ID. It is normally validated against a user providing a username and password. Upon completion of the GAFE authentication integration with Office 365 users of GAFE that have a corresponding Office 365 mailbox will login with the Office 365 username and password (same as logging into Active Directory). The diagram below is a simple representation of the authentication path.

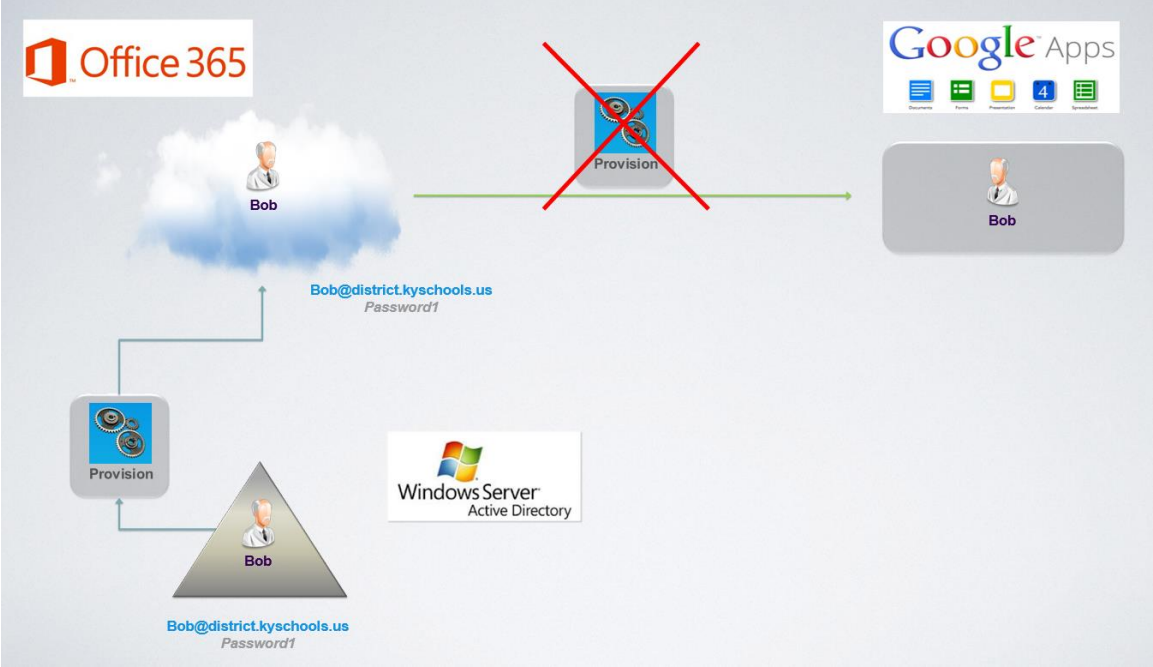
Diagram 2



Authorization defines what a given user has access to after login. Different systems can use a multitude of authentication validation methods, from group membership to robust claims-based information about the user. In this implementation of GAFE to Office 365 there will be no authorization information passed to the user from Office 365, meaning what the user has access to is defined in the Google Apps environment. Office 365 is used only to login them in, proving they are who they claim to be.

Provisioning is the automated creation of users, groups, etc from one system to another. This process can also modify or delete objects from the authoritative system to the relying system. There's a provisioning process in place today (OLPS) which provisions from Active Directory to Office 365 so districts don't have to perform common user management tasks in Office 365. At this moment there is NO technical option to provide user provisioning from Office 365 to Google Apps for Education. This is based on our current design in Office 365 which prevents the ability. This is being considered in future updates of Office 365 that could allow the provisioning ability but at the moment you should be aware this is not an option. At this time districts will continue to manage GAFE accounts in the Google Admin Console.

Diagram 3



Document Updates/Location

This document could be updated and enhanced over time. Please check for new versions periodically at http://education.ky.gov/districts/tech/Pages/Administration-andInstall-Guides.aspx

Document Feedback

If you have any recommendations to improve this guide please send your suggestions to KETSHelp@education.ky.gov and reference the location of this document.

Prerequisites

A Google Apps for Education (GAFE) space must be setup with the district email suffix as the GAFE domain. **Please note that existing accounts with a different suffix (i.e. a non-kyschools.us suffix) will be rendered inaccessible after this process!**

If Chromebook integration is desired, device management licenses must be purchased and devices must be enrolled. At this time, your district is a good candidate for Azure Active Directory implementation if you are using the "Guest" login functionality of the Chromebook. Your district is NOT a candidate if your district has a one to one implementation of Chromebooks or shared Chromebooks where the users login directly with their GAFE credentials.

*note – future work by Google will permit individual account login to a Chromebook with integrated SSO (Azure Active Directory username and passwords).

Setup GAFE to Office 365 SSO

Just reiterating, this configuration is for authentication from GAFE to Office 365 only. Account provisioning is not addressed at this time.

Step 1: Setup GAFE with the district email suffix domains (district.kyschools.us & stu.district.kyschools.us). Verify ownership of domains with support from the KETS Service Desk.

> * Best practice: set up ***district.kyschools.us*** as the main (primary) GAFE space and add the ***stu.district.kyschools.us*** as a domain in the Admin Console of the primary space.

Step 2: In the GAFE Admin Console create a temporary GAFE SuperAdmin account.

*Note: This account does not need to be created in Active Directory or Office 365; it's only used for the initial configuration in Google Apps. If the **GAFE SuperAdmin** account does have a corresponding Office 365 account you will still login with the GAFE password, even after the implementations of SSO to Office 365.*

Step 3: After Steps 1 and 2 are complete, you are ready to schedule a time to implement the integration.

You will need to specify *when* you'd like the setup to be completed. If you are already leveraging GAFE, your users will have a different login experience immediately following implementation of Azure Active Directory Single Sign-On (SSO). To ensure someone from the KETS Messaging and Directory Services (MADS) team is able to complete the work at your desired time, give a minimum of 24 hours of lead time.

> The KETS Service Desk Ticket should be submitted as an email to: ketshelp@education.ky.gov with the following subject line: ***GAFE Integration to Azure AD***. Contained within the body of the email should be the GAFE SuperAdmin account username, BUT not the

password. Upon connecting on the scheduled integration time, the account password can be shared.

Depending on the current district Google Apps implementation, there may need to be notifications of change of login for to all users.

Step 4: The MADS team will log in to your GAFE Admin Console. Configurations will be set for Single Sign On (SSO) with Azure Active Directory and an Azure Security Certificate will be imported.

Step 5: Upon notification of completion from the KETS Service Desk, the temporary GAFE SuperAdmin account should be removed/disabled/deleted.

Step 6: Ensure a 1:1 match with user accounts (UPN or SMTP address) in Active Directory and Google Apps for Education Admin Console.

Step 7: Test authentication with GAFE URLS (e.g. https://drive.google.com/a/stu.district.kyschools.us)

Step 8: If Chromebook authentication is desired, make sure devices are enrolled in the district Admin Console.

Step 9: Configure Single Sign On for Chrome Devices.

District Implementation

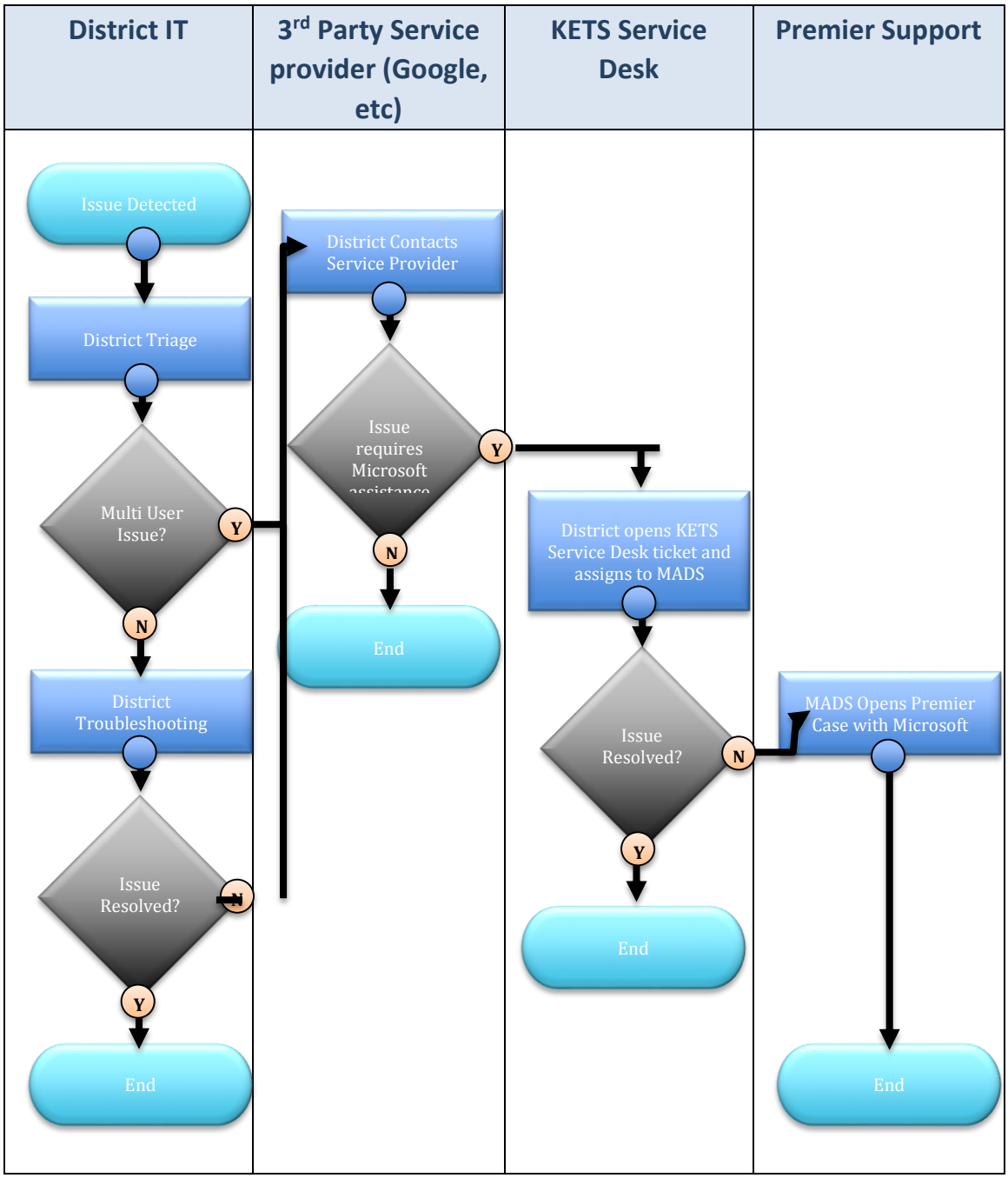
- For Single Sign-On, Google suggests sending users directly to the drive property first. The implementation or login URL would be: https://drive.google.com/a/*district*.kyschools.us
- If the desire is for a user to land on the UserHub, the implementation or login URL would be the pass-through Microsoft Online Login page. When a user completes successful login, the browser passes them on to the Google UserHub where all of the Google Apps properties are listed.

- iOS implementation – download the specific Google Apps (Drive, etc.) and sign in. User will need to sign in twice the initial time the app is authorized.
- Chromebook Guest user implementation – instruct users to use Chromebook as a guest user, then direct them to a login or launch button to Google Apps, per above instructions.

Supportability Framework

It is important to note and understand the supportability structures around the integration of 3rd Party applications with Azure Active Directory. The following notes should be consulted prior to initializing the integration request (Step 2 from above).

- The KDE has a Microsoft Premier Support Agreement that incorporates all integration activity within Azure Active Directory.
- If authentication into Office 365 webmail (https://portal.office.com) is successful, then Azure Active Directory is functioning as designed. In a general sense, Office 365 is leveraging Azure Active Directory from the same mechanism as additional 3rd party applications (e.g. Google Apps for Education). If the issue does not require Microsoft assistance (authentication into Office 365 is successful), district IT support should begin consulting the 3rd party app support channels.
- See the below triage and flow chart. For support details for Google Apps For Education (GAFE) see the "Support" tab inside of the GAFE Admin Console.


District IT
3rd Party Service provider (Google, etc)
KETS Service Desk
Premier Support
Issue Detected
District Triage
Multi User Issue?
Y
N
District Troubleshooting
Issue Resolved?
N
Y
End
District Contacts Service Provider
Issue requires Microsoft
Y
N
End
District opens KETS Service Desk ticket and assigns to MADS
Issue Resolved?
N
Y
End
MADS Opens Premier Case with Microsoft
End